CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method in a data processing system for maintaining multiple secure user private keys in a non-secure storage device, said method comprising the steps of:

establishing an encryption device having an encryption engine and a protected storage device, wherein said protected storage device is accessible only through said encryption engine;

establishing a master key pair for said system, said master key pair including a master private key and a master public key;

storing said master key pair in [[a]] said protected storage device;

establishing a unique user key pair for each of multiple users, each of said user key pairs including a user private key and a user public key;

said encryption engine encrypting each of said user private keys utilizing said master public key; [[and]]

storing each of said encrypted user private keys in said non-secure storage device, wherein each of said encrypted user private keys is secure while stored in said non-secure storage device;

in response to receiving a message to transmit to a recipient, said encryption engine decrypting a particular user's private key utilizing said master private key;

said encryption engine encrypting said message utilizing said decrypted particular user's private key and said recipient's public key; and

transmitting said encrypted message to said recipient.

2-4. (Cancelled)

5. (Previously Presented) The method according to claim 4, wherein the step of establishing a unique user key pair for each of multiple users further comprises the step of associating each said user key pair with an application.

6. (Previously Presented) The method according to claim 5, further comprising the steps of:

establishing a certificate, said certificate being associated with said application, said particular user's private key, and said particular user;

in response to said particular user attempting to access said application utilizing said certificate, said encryption engine utilizing said certificate to determine a location within said non-secure storage device for said particular user's private key associated with said certificate;

said encryption engine decrypting said particular user's private key; and

said encryption engine utilizing said decrypted particular user's private key to encrypt messages transmitted by said application.

7. (Previously Presented) The method according to claim 1, wherein said step of storing each of said encrypted user private keys in said non-secure storage further comprises the step of storing each of said encrypted user private keys in a hard drive.

8. (Previously Presented) The method according to claim 7, further comprising the step of each of said unique user key pairs being capable of being utilized only in said data processing system wherein a particular user key pair is established, wherein said particular user key pair is not capable of being utilized in a second data processing system.

9. (Currently Amended) A data processing system for maintaining multiple secure user private keys in a non-secure storage device, said data processing system comprising:

an encryption device ~~included within said system~~ for establishing a master key pair for said system~~, said master key pair including~~ that includes a master private key and a master public key, said encryption device including an encryption engine and a protected storage device for storing said master key pair wherein said protected storage device is capable of being accessed only through said encryption engine;

~~said master key pair including a master private key and a master public key;~~

~~a protected storage device for storing said master key pair;~~

said encryption device executing code for establishing a unique user key pair for each of multiple users, each of said user key pairs including a user private key and a user public key;

said encryption ~~device~~ engine executing code for encrypting each of said user private keys utilizing said master public key; [[and]]

a non-secure storage device for storing each of said encrypted user private keys, wherein each of said encrypted user private keys is secure while stored in said non-secure storage device[[.]];

wherein said encryption engine, responsive to receiving a message to transmit to a recipient, executes code for decrypting a particular user's private key utilizing said master private key and executes code for encrypting said message utilizing said decrypted particular user's private key and said recipient's public key; and

wherein said system transmits said encrypted message to said recipient.

10-12. (Cancelled)

13. (Previously Presented) The system according to claim 12, further comprising said system executing code for associating each said user key pair with an application.

14. (Previously Presented) The system according to claim 13, further comprising:

said system executing code for establishing a certificate, said certificate being associated with said application, said particular user's private key, and said particular user;

in response to said particular user attempting to access said application utilizing said certificate, said encryption engine executing code utilizing said certificate for determining a location within said non-secure storage device for said particular user's private key associated with said certificate;

said encryption engine executing code for decrypting said particular user's private key pair; and

said encryption engine capable of utilizing said decrypted particular user's private key to encrypt messages transmitted by said application.

15. (Previously Presented) The system according to claim 14, further comprising said system executing code for storing each of said encrypted user private keys in a hard drive.

16. (Previously Presented) The system according to claim 15, further comprising each of said unique user key pairs being capable of being utilized only in said data processing system wherein a particular user key pair is established, wherein said particular user key pair is not capable of being utilized in a second data processing system.

17. (Cancelled)